CYBERIUM ARENA

— SIMULATOR —

SYLLABUS

IOT EXPLOITATION

MAIN FEATURES

Labs

The labs hold questions and tasks to support the training.

Book

The coursebooks accompany the lecturers and students alike in cybersecurity studies.

Scenarios

Provide participants possible situations from cybersecurity or cyberterrorism to solve.

Project

Trainees must complete a practical built-in project, produce defense and assault tools.

CYBERIUM ARENA

SIMULATOR

Description

IoT or the Internet of Things is one of the most upcoming trends. The growth of IoT devices makes this training valuable to Blue and Red Teams, understanding where and how IoT operating systems can be exploited. This program is based on theoretical and practical vulnerabilities in IoT devices, architecture, identifying attack surfaces, and exploiting different IoT devices.

MODULES

Module 1: Intro to IoT Security

Finding IoT Device
Learning Shodan
Using Advanced API
Searching with CLI
Collecting and Extracting Data
Vulnerabilities
Nmap Basics
Banner Grabbing Techniques
Mapping the Internet
Metasploit

Module 2: Firmware Analysis

Fundamental Concepts
Setting your VM
Introduction to Embedded OS
Understanding Firmwares
Retrieving Firmwares
Attack Surface
Mapping IoT Attack Surface
Mounting File Systems
Identifying Hardcoded Secrets

Module 3: Embedded OS

Introduction to Embedded OS
Working with SquashFS
Detecting Default Password
Analyzing System Files
Emulating Firmware Binary
Working with QEMU
Deploying Firmadyne
Automating the Deployments
Weaponising Firmwares
Backdooring a Firmware

Module 4: Web Application IoT

Web application Security for IoT
Exploitation IoT with Burp
Exploitation IoT with Command Injection
Exploitation IoT with Blind Command Injection
Exploitation IoT with Brute-Force

Module 5: Software-Based Exploitation

Software Exploitation Techniques
Intro to MIPS
Binary Debugging
ARM Buffer Overflow
Exploitation with GDB on MIPS